eXtended Managed Detection and Response

Select from an array of leading security services partners to get proactive threat hunting, comprehensive alert management, and 24/7 incident response.

Security operations have become a never-ending battle of reviewing countless low-fidelity alerts and trying to proactively combat attackers. Struggling to keep up, security teams of all sizes have turned to managed security services to handle the volume of work generated by their siloed threat prevention and detection tools.

Business Benefits

- **Let our XMDR specialized partners focus on your business:** Reduce response times and improve security outcomes with dedicated experts monitoring your environment and investigating threats.
- **Boost your security maturity:** Gain a proactive SOC with 24/7 coverage, covering everything from alert management to incident response.
- **Go beyond managed EDR:** Get complete coverage across network, endpoint, and cloud data from many leading partners.
- **Make impactful security investments:** Free up investments with a predictable opex model, helping you bolster your security posture.
- **Benefit from in-depth security experience:** Get forensic expertise for threat hunting, investigation, and response.

Simplify Security Operations with our World-Class Cortex XMDR Specialized Partners

Our elite extended managed detection and response (XMDR) partners can help your team stop the most advanced attacks while reducing alert fatigue and analyst burnout. Plus, you can avoid the painstaking process of building or refining your own security operations centers (SOCs).

Palo Alto Networks has teamed up with industry-leading MDR service providers to offer the most comprehensive combination of experienced analysts, mature operational processes, and market-leading security products. These partnerships deliver:

- Best-in-class threat prevention from the Cortex XDR agent.
- Complete visibility, detection, and response across network, endpoint, and cloud assets with Cortex XDR.
- Expert threat hunting and forensic specialists who will reduce your mean time to detect (MTTD) and respond (MTTR).
- In-depth security experience to help you properly tune and manage dedicated infrastructure.

This represents a fundamental shift in the way MDR services are delivered—toward a focus on enabling positive outcomes and customer choice, not increasing the sales of point products. Traditional managed security services have focused on alert management and notification of critical threats, placing the onus of time-intensive investigations on the customer. MDR offerings from most technology vendors hide shortcomings of limited point products under the veil of services. This is evident in a lack of concrete detection and response service-level agreements (SLAs).

Instantly Scale Your Security Operations

Our hand-picked XMDR partners grant you instant access to their SOC teams and best practices in alert management, threat investigation, incident response, and threat hunting. Decades of experience mean expert deployment and fine-tuning of Cortex XDR for each environment, providing a mature SOC in days, not years.

Our XMDR partners scale with you as your organization grows. Traditional approaches consistently require the addition of security analysts, technology, and operational process to stay ahead of new risks. Our XMDR partners simply require your latest employee count, and their services expand to keep risk in check—all handled for you.

Powered by Cortex XDR Technology

Cortex® XDR™ is the industry's first extended detection and response platform that natively integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations like yours secure their digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

In a market flooded with detection and response technology, our XMDR partners selected Cortex XDR to power their services. Providing the best-combined protection and visibility in the 2021 MITRE ATT&CK® evaluation, Cortex XDR allows our XMDR partners to deliver the best detection and response services in the market. This partnership of best-in-class technology with security services ensures customers realize positive security outcomes across all threat vectors, not just the endpoints.

Key Capabilities Across Our XMDR Specialized Partners

24/7 Year-Round Coverage

Instantly mature to a proactive SOC. Maintaining staff for continuous coverage is difficult and costly. Our partners provide around-the-clock coverage of your environment with expert analysts who manage alerts, proactively hunt threats, and respond in accordance with your SLAs.

Alert Detection and Triage

Reduce detection times by combining AI-powered analytics from Cortex XDR with world-class threat hunters and analysts from our XMDR partners. On average, security teams look at less than 7% of their alerts, addressing only the most critical alerts. Many of our XMDR partners combine automation and orchestration with human expertise to ensure no threat goes unchecked.

Lightning-Fast Investigation and Response

Stop attacks before the damage is done with dedicated and experienced analysts. Many security teams today do not have the resources to investigate complex, multistage attacks. Backed by Cortex XDR, our partners' forensic analysts investigate threats with speed and precision, defining an attack's root cause, scope, and trajectory for targeted response.

Enrichment

Bolster your security with global intelligence. Gathering and maintaining intelligence to aid detection and investigations requires dedicated personnel. Our XMDR partners use their experiences across customers around the world, in every industry, to steadily improve detection and response times. By natively integrating threat intelligence feeds with shared analyst experiences, every customer is protected from today's emerging threats.

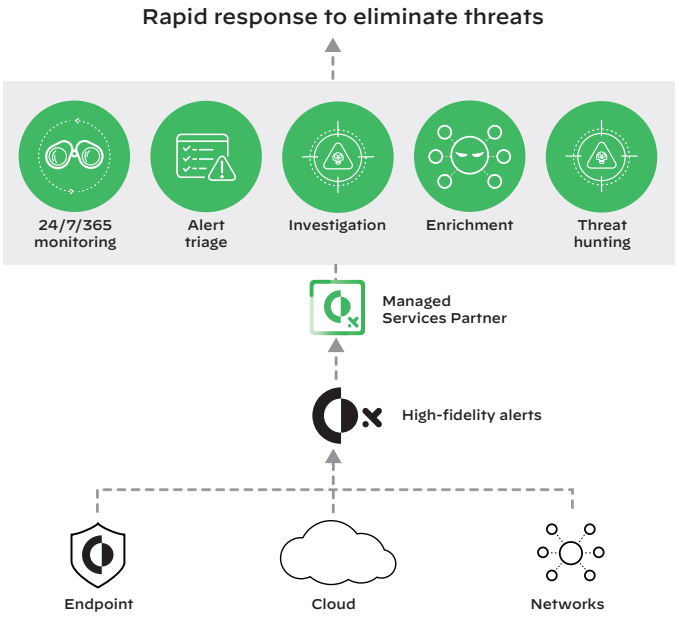

Figure 1: Overview of our partners' XMDR services benefits

Threat Hunting

Leverage dedicated, proactive threat hunters. Even organizations with established SOCs struggle to find people and time for threat hunting. Benefit from our partners' scale and visibility across varying industries, with instant access to dedicated threat hunters, experienced at finding today's stealthiest attacks.

Table 1: All the Benefits of Cortex XDR and XMDR Services

Value	Cortex XDR	With XMDR*
Prevention from malware, exploits, ransomware, and fileless threats	✓	✓
Automated, machine-learning-based detection	✓	✓
Custom rules	✓	✓
Root cause analysis	✓	✓
Network, endpoint, and cloud prevention	✓	✓
Live response	✓	✓
Incident grouping	✓	✓
24/7 expert security analysis	—	✓
Investigation of every alert	—	✓
Focused incident analysis	—	✓
Dedicated, proactive threat hunters	—	✓
Guided remediation actions	—	✓
Direct access to analysts	—	✓

* Benefits and capabilities may vary by XMDR partner. Please contact your XMDR specialized partner to verify the services they provide.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com